RESEARCH ARTICLE OPEN ACCESS

Network Intrusion Detection System

Gopalkrishna N. Prabhu, Kushank Jain, Nandan Lawande, Narendra Kumar,Yashasvi Zutshi, Rohan Singh, Jyoti Chinchole
Department of Information Technology, Atharva College of Engineering, University of Mumbai, India

ABSTRACT
Attacks on computers and data networks have become a regular and sophisticated issue. Intrusion detection has shifted its attention from hosts and operating systems to networks and has become a way to provide a sense of security to these networks. The aim of intrusion detection is to detect misuse and unauthorized use of the computer systems by internal and external elements. Typically, Intrusion Detection Systems allow statistical anomaly and rule-based misuse models to detect intrusions as the behavior of the intruding element is considered to be different from the authorized user behavior.

Keywords-- Denial of Service (DOS),Intrusion Detection System (IDS), Network Intrusion Detection System (NIDS), Unified Modelling Language (UML)

I. INTRODUCTION

An intrusion detection system (IDS) is a software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. It is neither required nor expected of a monitoring system to stop an intrusion attempt. The typical work of IDS is to record information related to observed events, notify the security administrators of important observed events, and generate reports, as in [1]. Many IDS also detect a threat and attempt to prevent it from succeeding. Several response techniques are used, wherein IDS stops the attack itself, changes the security environment (e.g., reconfiguring a firewall), or changes the attack's content. A more accurate definition of intrusion detection system can be found in [2] which define intrusion detection systems to detect intrusion in the form of unauthorized uses, misuses, or system abuses by authorized users or external perpetrators. Today, in this world of Internet it is essential for each network user to have some security over the network for the purpose of communication or data transfer. Reference [3] shows providing security of data and continuously maintaining the services provided by a network is the objective of an intrusion detection system. There are many security systems on the network that provide security from viruses or harmful file extensions. The space provided varies from system to system. The commonly used network securities are firewall, anti-viruses and so on. And each of these security software provide different services to NETWORK user. So there is a great need of a comfortable SECURITY access for the systems which are connected in a network or for seeking any information on daily basis through the systems that are connected through LAN or even on internet. A "Network Intrusion Detection System (NIDS)" does the work of monitoring network traffic, looking for suspicious activity that can be an attack or unauthorized activity. A large NIDS server can be set up on a supporting network, to monitor traffic; also to monitor traffic for a particular switch, server, gateway, or router smaller systems can be set up. A NIDS server can also scan system files looking for unauthorized activity and to maintain data and file integrity, in addition to monitoring incoming and outgoing network traffic. The NIDS server can also detect changes in the server core components. A NIDS server can also look for suspicious traffic or usage patterns that match a typical network compromise or a remote hacking attempt and scan server log files. The NIDS server can also serve a proactive role instead of a protective or reactive function. It can be used to include for scanning live traffic to see what is actually going on or scanning local firewalls or network servers for potential exploits.

A NIDS server does not replace basic security such as encryption, firewalls, and other authentication methods. The NIDS server is a backup network integrity device. Neither system (primary or security and NIDS server) should replace common precaution.

Network-based intrusion detection systems (NIDS) monitor traffic passing through a network and compare that traffic with a database of so called signatures known to be associated with suspicious activity. Different signature types used by the typical NIDS are as follows:

- Header Signatures - Scans the header portion of network packets to identify suspicious or

inappropriate information.

- Port Signatures - Monitors the destination port of network packets to identify packets destined for ports not serviced by the servers on the network, or targeting ports known to be used by common attacks.
- String signatures - Identifies strings contained in the payload of network packets to identify strings known to be present in malicious code.

A NIDS will typically only pick up packets to which it is attached, traveling in the network segment. NIDS are generally placed in between an internal network and the firewall, to ensure that all inbound and outbound traffic is monitored. In addition, if the network-based IDS software is installed on a computer it is vital that the computer be equipped with a network interface card (NIC) which supports promiscuous mode so that it is able to capture all network packets and not only those that have that IP address as its destination.

II. TYPES OF ATTACKS

From the point of view of intrusion detection and response, we need to observe and analyze the anomalies due to both the consequence and technique of an attack. The technique can help identify the attacker, if the consequence gives an idea about the type of the attack.

Categories of attacks according to their consequences are as follows:

- Black hole: All traffic is redirected to a specific node, which may not forward any traffic at all.
- Routing Loop: In a route path a loop is introduced.
- Network Partition: Here the nodes in different sub networks cannot communicate even though a route between them actually does exist and a connected network is partitioned into k (k >= 2) sub networks.
- Selfishness: A node does not serve as a relay to other nodes.
- Sleep Deprivation: A nodes battery power is forced to get exhausted.
- Denial-of-Service: The source node is denied services of receiving and sending data packets to its destinations.

III. DIFFERENT APPROACHES TO INTRUSION DETECTION

Intrusion Detection is typically grouped into two categories, as in [4], [5]:

- Host-based IDS - Host-based IDS monitors the activity on individual systems with a view to identifying unauthorized or suspicious activity taking place on the operating system.
- Network-based IDS - Network-based IDS is solely concerned with the activity taking place on a network (or more specifically, the segment of a network on which it is operating).

Network Intrusion Detection can be approached as either Knowledge-based or Behavior-based categories, as in [6]:

- Knowledge-based for Misuse Detections- Includes a database of signatures known to be associated with malicious or unauthorized activity. Comparison of activity data against the signature database is done and when a match is identified, response is generated.
- Behavior-based for Anomaly Detections- Monitors for deviations from the normal operation of systems or networks based on knowledge gathered over time of the normal usage patterns of users and systems

IV. DESCRIPTION OF THE PROPOSED DESIGN OF INTRUSION DETECTION SYSTEM

4.1 Use-Case Diagram:

Explanation of use – case diagram in Fig.1:

- First the user receives the incoming packets from the internet.
- Then the received packets are examined by matching with the manual virus database with the help of NIDS software.
- If the packets contain the viruses which are in the manual database then these packets are called as infected packets.
- Authentication of static IP addresses can also be done by the user by adding the IP addresses to the database of authenticated IP addresses.

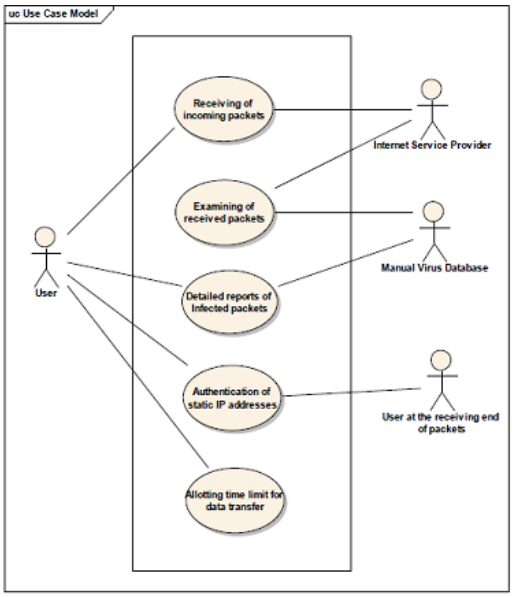

Fig. 1 Use-Case diagram of the proposed design of Intrusion Detection System

4.2 Sequence Diagram:

Explanation of sequence diagram in Fig.2:

- The sequence diagram shows the flow of the project in a proper sequence.
- First the user sends the downloading request to the internet to download the packets.
- Then the examining of the received packets is done by the manual virus database.
- If the packets are infected the detailed report of the infected packets are sent to the user.

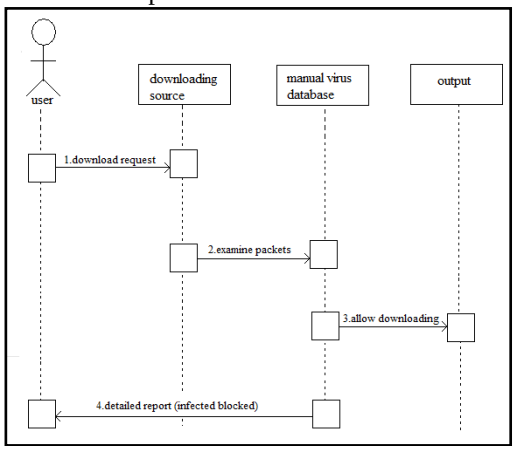

Fig. 2 Sequence diagram of the proposed design of Intrusion Detection System

4.3 AttacksinConcernbytheimplementedSystem:

4.3.1 Man-In-The-Middle: The most advanced type of attack on a wireless or wired network is the "Man-In-The-Middle" attack. The attacker attempts to insert between the user and an access point as the middleman. The aggressor then proceeds to collect logs on information while forwarding information between the user and access point. As a result, the attacker can modify data by malicious interception.

4.3.2 Ping of Death: On the Internet, ping of death is a denial of service (DOS) attack caused by an IP packet larger than the 65,536 bytes allowed by the IP protocol which an attacker deliberately sends. A feature of TCP/IP is fragmentation; it allows breaking of a single IP packet into smaller segments. In 1990s, attackers began to take advantage of that feature when they found that a packet broken down into fragments could add up to more than the allowed 65,536 bytes. Various operating systems froze, crashed, or rebooted as they didn't know what to do when they received an oversized packet.

4.3.3 Denial-of-Service: A denial of service occurs when an attacker has engaged most of the resources a host or network has available, rendering it unavailable to legitimate users. This sort of attack specifically targets the availability of the network i.e. by blocking network access, causing excessive delays, consuming valuable network resources, etc.

4.4 Location of NIDS in the System:

The different locationsofthenetworkintrusiondetection aredepictedinFigure3.

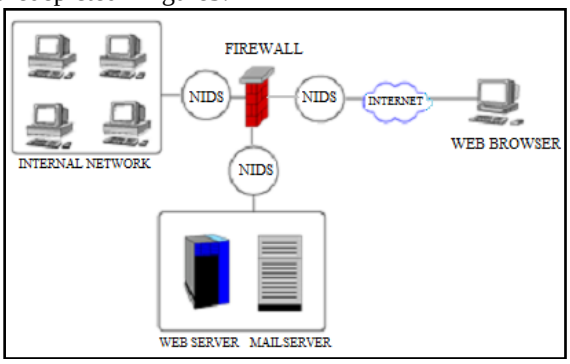

Fig. 3 Different Locations of the proposed Network Intrusion Detection System

4.5 Platform Description:

The developed network intrusion detection system is tested on x86 architecture machines. The programming language chosen is Java. This is inspired by literature in the field of network intrusion detection development in such a language.

V. ARCHITECTURE GLOBALLY PROPOSED

Regardless of the type of IDS there are a few common components that typically constitute IDS:

- Traffic Collector - The component is responsible for gathering activity and event data for analysis. On a host-based ID this will typically include metrics such as inbound and outbound traffic and log and audit file activity recorded by the operating system. A NIDS will analyze the segment of the network by pulling the data off.
- Analysis Engine - The analysis engine analyzes the data that the traffic collector gathers. In case of a knowledge-based IDS comparison of data is done with a signature database. A behavior-based IDS, compares it against normal behavior information gathered over time to see if the current behavior deviates from the norm.
- Signature Database - Used in knowledge-based systems, the signature database is an amalgamation of signatures known to be associated with suspicious and malicious activities. A knowledge based IDS is only as good as its database.
- Management and Reporting Interface - A management interface providing a mechanism by which system administrators may manage the system and receive alerts when intrusions are detected

VI. IMPLEMENTATION

6.1 Implementation Outline:

The proposed Network Intrusion Detection System is implemented according to the following steps, as in [7]:

1) Listening to the network and capturing the packets: The first step is to develop a sniffer. Each system, having an Ethernet network has a network card with its own physical address. The network card examines each packet over the network and captures it once intended to the host machine.
2) Decoding the packets: The sniffer sends all packets one after another to the decoder and finds their category. For example, if the packet received is TCP, the decoder collects its source and destination addresses and ports, TCP flag and data field.
3) Detecting the specific attacks: The attacks to be detected by the proposed NIDS are Man-in-the-Middle, DOS and ping of death.
4) Heuristic Detection process: Signature database is stored and scanned for detecting the intrusions.
5) Output Module: The output module is executed once the NIDS detects an intrusion to inform record and notify the attack.

6.2 Graphic User Interface (GUI):

The GUI of the proposed Network Intrusion Detection System is as shown figure 4.

VII. CONCLUSION

The proposed network intrusion detection system is extensible and portable and much other functionality can be implemented. Regardless, it does present certain drawbacks. The system proposed takes into account the scenario approach.

It is a difficult task to evaluate intrusion detection system. It is impossible to detect all possible intrusions that might occur where a certain intrusion detection system is located and assigned. Firstly, there are numerous intrusion techniques, as in [8]. Secondly, the site may not possess information about previous intrusions detected at other sites. Also, new intrusion techniques can be employed by intruders in the computer system on discovering previously unknown vulnerabilities in it. Reference [7] shows the evaluation of an intrusion detection system also becomes difficult as, where it usually detects a certain intrusion; it may remain unsuccessful in detecting similar intrusions when the systems total level of computing activity is high. This complicates the task of thoroughly testing the intrusion detection system.

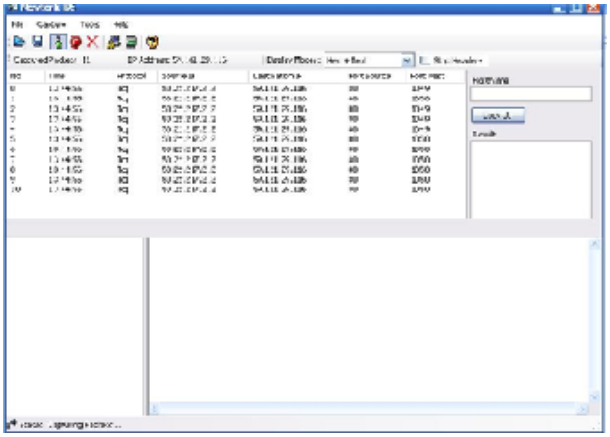

Fig. 4 Graphic User Interface of the proposed Network Intrusion Detection System

REFERENCES

[1] R.G.Bace, "IntrusionDetection", TechnicalPublishing,1995.
[2] B. Mukherjee et al., "Network intrusion detection", IEEE Network, vol.8,no.3,pp.26–41,1994.
[3] K.Ramamohanaraoetal., "Thecurseofeaseofaccesstotheinternet," 3rdInternationalConferenceonInformationSystemsSecurity.
[4] ITL Bulletin "Acquiring and Deploying Intrusion Detection Systems" Nov. 1999.
[5] K.K.Gupta,"Robustandefficient intrusiondetectionsystems",Ph.D. dissertation,TheUniversityof Melbourne,Departmentof Computer ScienceandSoftwareEngineering,January2009.
[6] M.A.Aydinetal.,"Ahybridintrusiondetectionsystemdesignfor computer network security", Computer and Electrical Engineering, vol.35,pp.517–526,2009
[7] EugèneC.Ezin,HervéAkakpoDjihountry, "Java-BasedIntrusionDetectionSystemina Wired Network",](IJCSIS) International Journal of Computer Science and Information Security, vol. 9, No. 11, November 2011.
[8] P.G.Neumann andD.Parker,"Asummary ofcomputer misuse techniques", in12thNationalComputerSecurity Conference,Baltimore, MD,1989,pp.396–407.